A Study on Provable Security of Signature Schemes for Multiple Signers

著者	矢内 直人
その他のタイトル	多人数署名の証明可能安全性に関する研究
学位授与大学	筑波大学 (University of Tsukuba)
学位授与年度	2013
報告番号	12102甲第6856号
URL	http://hdl.handle.net/2241/00122384

(博甲)

氏　名（本籍）	矢内　直人（岩手県）
学位の種類	博　士（工　学）
学位記番号	博　甲　第　6856　号
学位授与年月日	平成２６年　３月２５日
学位授与の要件	学位規則第４条第１項該当
審査研究科	システム情報工学研究科
学位論文題目	A Study on Provable Security of Signature Schemes for Multiple Signers （多人数署名の証明可能安全性に関する研究）

主　査	筑波大学　教授	工学博士	岡本　栄司
副　査	金沢大学　教授	博士(工学)	満保　雅浩
副　査	筑波大学　准教授	工学博士	片岸　一起
副　査	筑波大学　准教授	博士(工学)	西出　隆志
副　査	筑波大学　助教	博士(理学)	金山　直樹

論　文　の　要　旨

本論文では電子署名技術の一般化に向けて、多人数ユーザ環境における証明可能安全な電子署名技術に関して研究を行っている。論文の第 1 章では実際の事例を基に研究の背景および目的について、2 章では関連する数学的知識および関連研究について述べ、第 3 章から第 7 章はユースケースごとに応じて設計された多重署名の提案方式が述べられている。第 3 章では DoS 攻撃やネットワーク欠損検出などネットワーク技術を視野に入れた Ordered Multisignature が、第 4 章では著作権管理システムを捉えた Structured Multisignature が、第 5 章ではルーティングセキュリティに特化した BGP-Aiding Aggregate Signature が、第 6 章では認証連携システムやプロバイダへの信頼担保を考慮した Certificateless Aggregate Signature がそれぞれ提案されている。既存方式では安全性の議論のみに焦点が当てられており、現実に求められる仕様や要件に注目されていなかった。この問題点に対し、本論文では安全性の要件を再考察し、標準的な仮定に基づく安全性と実用性を備えた方式を提案している。また、これらの提案を通じて、第 7 章では電子署名を一般化した Unrestricted Aggregate Signature を提案している。第 3 章から第 6 章の方式は第 7 章の方式を各ユースケースで最適化した方式とみなすことができる。ベースとなっているのは Unrestricted Aggregate Signature の安全性証明に必要となる数学的性質である。その性質とは Programmable Hash Function と Re-randomization であり、実際にこの性質を持つ方式が証明可能安全であることを示している。この知見はこれまで未解明であった電子署名の一般化につながるものである。第 8 章では本論文の研究をまとめ、今後の課題について述べている。

審　査　の　要　旨

【批評】

本論文では、ディジタル署名が組織などで必須となることを念頭にして、多人数ユーザ環境における証明可能安全な電子署名技術に関して研究を行っている。特に重視されるのは安全性であるため、まず、Unrestricted Aggregate Signature の安全性証明に必要となる数学的基盤として Programmable Hash Function と Re-randomization の性質を明らかにし、実際にこの性質を持つ方式が証明可能安全であることを示している。そして、この結果をもとにいくつかのユースケースに適した方式を各々提案している。

以上、本論文は、多重署名の理論基盤をあたえるだけでなく、応用的にも優れた成果となっており、博士論文にふさわしい成果であるとみられる。

【最終試験の結果】

平成 26 年 2 月 5 日、システム情報工学研究科において、学位論文審査委員の全員出席のもと、著者に論文について説明を求め、関連事項につき質疑応答を行った。この結果とリスク工学専攻における達成度評価による結果に基づき、学位論文審査委員全員によって、合格と判定された。

【結論】

上記の学位論文審査ならびに最終試験の結果に基づき、著者は博士（工学）の学位を受けるに十分な資格を有するものと認める。